IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION

DONNA CURLING, ET AL., **Plaintiffs,** **v.** **BRAD RAFFENSPERGER, ET AL.,** **Defendants.**	**DECLARATION OF J. ALEX HALDERMAN IN SUPPORT OF CURLING PLAINTIFFS' REPLY IN SUPPORT OF MOTION FOR PRELIMINARY INJUNCTION** **Civil Action No. 1:17-CV-2989-AT**

Pursuant to 28 U.S.C. § 1746, J. ALEX HALDERMAN declares under penalty of perjury that the following is true and correct:

1. I hereby incorporate my previous declarations as if fully stated herein. I have personal knowledge of the facts in this declaration and, if called to testify as a witness, I would testify under oath to these facts.

2. Georgia's new voting system incorporates optical scanners and ballot marking devices ("BMDs") manufactured by Dominion Voting Systems, Inc. ("Dominion"). Under this system (the "BMD voting system"), all in-person voters will select candidates on BMDs; the BMDs will print a paper ballot that is supposed to contain the voter's selections in both human-readable text and as a machine-

readable barcode;[1] the voter will insert the paper ballot into an optical scanner, which will store a digital scan of the printout;[2] the scanner will process the barcode and count the votes encoded in it;[3] and the paper ballots will be retained for use in audits or recounts. Absentee voters will not use BMDs but will instead complete hand-marked paper ballots ("HMPBs"), which will be counted by similar optical scanners.

3. Despite the addition of a paper trail, the BMD voting system suffers from serious security risks that are similar to the risks of Georgia's old paperless DRE voting system. Neither the DRE system nor the BMD system can achieve the level of security necessary to withstand an attack by a sophisticated adversary, such as a hostile foreign government. As I will explain, BMDs are vulnerable to serious attacks that have the potential to change all records of the vote. Moreover, when BMDs are used by all in-person voters, as in Georgia, there is a high risk that attackers could exploit them to change an election outcome.

---

[1] Specifically, QR codes, a kind of matrix barcode. QR codes differ from one-dimensional barcodes most relevantly in that they store more data in the same amount of space. For technical details about QR codes, see the international standard that defines them, *ISO/IEC 18004:2015: Information technology - Automatic identification and data capture techniques - QR Code bar code symbology specification*, available at https://www.iso.org/standard/62021.html.

[2] Decl. of Dr. Eric Coomer, Dckt. 658-2, at 10.

[3] Id. at 9.

4. However, Georgia can greatly strengthen the security of future elections through a straightforward procedural change. Rather than directing all in-person voters to use BMDs, the State could have in-person voters mark paper ballots by hand and reserve BMDs for voters who request to use them. This approach would require no additional equipment and would result in no loss in accessibility. Hand-marked paper ballots are already used in Georgia for absentee voting, and so they are prepared and printed for every ballot style in every election. The state's new optical scanners are already capable of counting hand-marked ballots.[4] BMDs would continue to be available for voters who need them. Yet the risk that election outcomes could be hacked would be *far less* than under Georgia's planned system.

5. Georgia is an outlier in adopting BMDs for all voters. Only 403 counties in the United States have done so, and almost 40% of them are in Georgia.[5] In contrast, the majority of election jurisdictions across the U.S. (representing nearly two-thirds of registered voters) provide BMDs exclusively for voters who request them (e.g., those with disabilities), which is much safer.

[4] Id.
[5] Stewart Decl. Ex. 2.

Hacking Risks Under the BMD Voting System

6. Georgia's new voting system relies on two kinds of equipment to cast and count votes: optical scanners and BMDs. The optical scanners could potentially be hacked to make them count inaccurately. However, such an attack *on the scanners* could be caught and corrected by manually inspecting the paper ballots in an appropriate recount or a sufficiently rigorous risk-limiting audit ("RLA").

7. Alternatively, attackers could hack the BMDs and cause them to print ballots that do not reflect voters' selections.[6] Such a hack could change both the text and the barcode on the printed ballots. Recounts or RLAs would not be able to detect this fraud, since all records of the vote, including the paper trail, would be wrong.

8. Defendants' experts do not dispute that BMDs can be hacked.[7] Like Georgia's legacy DREs, the new BMDs are computers, they run outdated and vulnerable software,[8] and they must be programmed using the State's election management system before every election. Attackers could potentially infect

[6] It is extremely dangerous to think of BMDs as "nothing more than an ink pen", as Defendants' expert Dr. Gilbert suggests (Decl. of Juan E. Gilbert, Dckt. 658-3, at 60). Unlike a pen, the BMDs used in Georgia are fully reprogrammable computers that might be infected by malicious software created by hostile foreign governments.
[7] Coomer decl. at 13; Gilbert decl. at 44.
[8] Decl. of J. A. Halderman, Oct. 2, 2019, at 22.

Georgia's BMDs with malware by spreading it from the election management system (EMS), in the same way that malware could have spread through the old DRE system.

9. Despite the use of new scanners and BMDs and a new EMS, Georgia's BMD-based voting system is at heightened risk of attack because of the legacy of poor security in the old DRE voting system and associated computer systems and networks. If nation state attackers infiltrated the old system, they likely did so by first infiltrating components such as the Secretary of State's computer network, the voter registration database software developed by PCC, Inc., and the non-"air gapped" computers used by state and county workers and outside contractors to transfer data into and out of the EMS. The record in this matter contains abundant evidence about vulnerabilities in all these components, some of which were unmitigated for years and may still be unmitigated. Responsibility for their security continues to rest with many of the same technicians and managers who oversaw the security of the old system and were unable or unwilling to implement effective security measures.

10. If attackers breached any of these components to attack the old voting system, those attackers may continue to have access. All these components will continue to be used with the new voting system, including to process data that is copied to polling place equipment. Technologies that State Defendants highlight as key defenses, such as anti-malware scans, anti-virus scans, and endpoint protection,

provide little defense against sophisticated attackers like hostile governments. As a result, the new election system continues to face a very serious risk of attack.

11. An attacker who infected Georgia's BMDs with malware could change the printed ballots in several ways. On a fraction of the ballots, the attacker could cause the human-readable text, the barcode, or both to reflect fraudulent choices determined by the attacker, rather than the voter's selections. I will discuss two kinds of such misprinting attacks below: attacks that change only the barcode and attacks that change both the barcode and the text.

Attack 1: Misprinting Only the Barcode

12. One kind of misprinting attack is a barcode-only attack. In this attack, malware would change a fraction of the BMD printouts so that they correctly showed the voter's selections in the ballot text but encoded a different, fraudulent set of selections in the barcode.

13. If an attacker changes only the barcode, it would be impossible for voters to detect the fraud. Voters cannot read the barcodes, so there is no practical way for voters to verify that the barcodes on their ballots match their intended selections. Moreover, when scanning BMD ballots, the optical scanners count only the votes encoded in the barcodes and ignore the text entirely. This means that voters cannot verify the portion of their ballots that gets counted.

14. Barcode misprinting attacks cannot be reliably detected using pre-election testing or parallel testing.[9] An attacker could decide which ballots to modify based on a very large number of variables, including the time of day, the number of ballots cast, the voter's selections, and whether the voter used options such as a large font size or an audio ballot. It is impossible for any practical amount of testing to examine all sets of conditions under which attackers might choose to cheat.

15. Officials could potentially detect a mismatch between the barcodes and the ballot text using a sufficiently rigorous post-election audit. However, Georgia has not announced plans to perform any kind of audit that would compare the barcodes and the printed text, nor what specific measures would be taken to render any potential audit sufficiently comprehensive and reliable. For example, while RLAs could potentially uncover barcode-only attacks, RLAs typically are designed to achieve a low risk-limit in specific races, but an attacker could target any race in any election. A barcode-only attack would likely not be detected in an RLA if it occurred in a race for which the RLA had a high effective risk-limit. Although some Georgia

[9] Philip B. Stark, "There is no Reliable Way to Detect Hacked Ballot-Marking Devices" (2019), available at https://www.stat.berkeley.edu/~stark/Preprints/bmd-p19.pdf.

counties recently conducted small-scale audit pilots,[10] these audits achieved a low risk-limit only in specific local races. The State has not announced plans to perform RLAs of any state-wide race in 2020.

16. Even if officials did detect that some ballots showed different choices in the barcode than in the text, there might be no way to determine the correct election results, contrary to the assertions of Defendants' expert, Dr. Juan Gilbert.[11] If the discrepancies resulted from an attack, this would cast doubt on *both* the barcodes and the ballot text. An attacker who was able to alter the barcode would be equally capable of altering the ballot text. Malware might even be designed to sometimes alter only the barcode and sometimes only the text. This means that officials could not simply ignore the barcodes and count only the text if they suspected the BMDs had been compromised. Rather than removing ambiguity from the record of voters' choices, as Dr. Gilbert claims,[12] BMDs with barcodes introduce a new source of it.

17. BMDs do not need to use barcodes. Several kinds of modern, EAC-certified BMDs deployed in other states do not use barcodes to encode votes. These

[10] "Risk-limiting audit concludes paper-ballot system accurate" (Nov. 13, 2019), available at https://sos.ga.gov/index.php/elections/risk-limiting_audit_concludes_paper-ballot_system_accurate.
[11] Gilbert decl. at 39(G).
[12] Id. at 39(C).

include the ClearBallot Clear Access system[13] and the Hart Verity Touch Writer.[14] Instead of a barcode for vote tabulation, these systems print a ballot that looks like a hand-marked paper ballot but has scan targets filled in for the selected candidates.

Attack 2: Misprinting Both the Barcode and the Text

18. As Dr. Gilbert points out, "[t]he primary goal of having a paper ballot is to enable an audit to ensure the integrity of the election; therefore, the audit or manual recount is the final say in the election outcome. If the auditability of the ballots is compromised, then the audit/recount fails."[15]

19. BMDs make it possible for an attacker to compromise the auditability of the ballots and thereby undermine the primary goal of the paper trail. Malware could cause the BMDs to print fraudulent selections in *both* the barcode and the human-readable text. This attack would be impossible to detect by auditing the ballots, even with an RLA, because all records of the voter's intent would be wrong. Pre-election testing and parallel testing also cannot reliably detect such cheating.

20. Unlike the security of hand-marked paper ballots, the security of BMD-printed ballots relies critically on voters themselves. The only practical way to

[13] https://clearballot.com/products/clear-access.
[14] https://www.hartintercivic.com/wp-content/uploads/VerityTouchWriter.pdf.
[15] Gilbert decl. at 39(B).

discover a BMD attack that altered both the barcodes and the ballot text would be if enough voters reviewed their ballots, noticed the errors, and alerted election officials.

21. Even if some voters do notice that their ballots were misprinted, the voters would have no way to prove that the BMDs were at fault. From an election official's perspective, the reporting voters might be mistaken or lying. Many voters would need to report that the BMDs misprinted their ballots before officials could be sure there was a systemic problem. And even then, there are no protocols or policies in Georgia that I have found that address how many voter complaints, or other conditions, involving BMDs would be required within or across polling places to support a finding—or even a robust investigation—of a systemic problem.

22. If officials did suspect that the BMDs had been attacked, there would be no straightforward way to respond or recover. One possible response would be to delay certifying the election results and conduct a forensic analysis to understand why ballots were misprinted and how many BMDs and votes were affected. Such an analysis might take months and would not be guaranteed to uncover a sophisticated attack. Even if an attack was confirmed, there is little chance that its effects could be undone. Research shows that voters fail to detect most misprinted ballots, and so the number of problem reports would likely be much smaller than the number of votes

that had been changed. The only recourse might be to rerun the election, which could be statewide involving millions of voters across Georgia.

Voter Verification Provides Insufficient Protection, Especially with Barcodes

23. Election experts have had widely varying intuitions about how likely voters are to detect errors in BMD printouts, which is why it is important to evaluate such issues and test such intuitions with appropriate experiments and studies. Last year, the National Academies of Sciences, Engineering, and Medicine called for research on this question, to "determine voter practices regarding the verification of ballot marking device–generated ballots and the likelihood that voters, both with and without disabilities, will recognize errors or omissions."[16] Subsequently, two studies have examined voters' verification performance using different methodologies. The results show that most voters do not review their BMD printouts, and that voters will likely fail to detect a large majority of errors caused by a BMD attack. This means that a BMD paper trail is not a reliable record of the votes expressed by the voters.

24. The first study observed voters in two polling places during a real election in Sevier County, Tennessee, which uses BMDs similar to Georgia's.[17]

[16] National Academies of Sciences, Engineering, and Medicine, *Securing the Vote: Protecting American Democracy* (2018). Available at http://nap.edu/25120.
[17] R. DeMillo, R. Kadel, and M. Marks, "What voters are asked to verify affects ballot verification: A quantitative analysis of voters' memories of their ballots" (2018). Available at https://ssrn.com/abstract=3292208.

Nearly half of voters did not review the BMD printout *at all*, and those who did review it spent an average of only 4 seconds doing so. This suggests that voters are likely to detect at most about half of misprinted ballots, and possibly far fewer.

25. A second study, conducted by my research group at the University of Michigan, measured the rate at which voters detected errors during a realistic simulated election. The voters used BMDs that we hacked so that one selection on each printout was wrong. We recorded how many participants reviewed their ballots and how many noticed the error and reported it to a poll worker. Our study has undergone peer review and has been accepted to appear at the IEEE Symposium on Security and Privacy,[18] which is the most selective top-tier publication venue for security research.[19] It will be published in early January.

26. In the first part of the study, subjects were not prompted to review their ballots in any way. Under that condition, 60% of voters failed to review their ballots, and voters only reported 6.6% of errors. Considering only prominent "top of the ticket" races, voters reported 14% of errors. These results imply that for every voter

[18] IEEE TC on Security & Privacy, "41st IEEE Symposium on Security and Privacy" (2019). https://www.ieee-security.org/TC/SP2020/.
[19] Guofei Gu, "Computer Security Conference Ranking and Statistics." Available at: http://faculty.cs.tamu.edu/guofei/sec_conf_stat.htm (accessed Dec. 12, 2019).

who notices that their ballot is misprinted and corrects it, there will likely be many more voters who fail to notice and have their votes stolen by the attacker.

27. In the second part of the study, we tested a variety of procedural changes to see whether they improved verification. Signage instructing voters to verify their ballots (as required in Georgia by H.B. 316) did not increase error reporting. Other changes did help, but only to a limited extent. For example, when a poll worker verbally prompted the voter to review the ballot after it was printed, voters reported 15% of errors. In my opinion, it is unlikely that any purely procedural changes can enhance voters' error detection rates sufficiently to stop outcome-changing fraud in close elections when BMDs are used by all in-person voters. And, as I have explained, barcodes make the problem even worse, by making it impossible for voters to notice or report some kinds of outcome-changing fraud.

28. Future BMD designs might achieve better error detection. I understand that Defendants' expert Dr. Gilbert has developed his own prototype of a new BMD system that is designed to enhance verification. Dr. Gilbert's improved design looks very different from Georgia's BMDs. It uses a transparent display that is overlaid on top of the paper printout and allows voters to see immediately whether the printout matches their on-screen selections. This innovation is evidently motivated by the poor verifiability of existing BMDs such as the ones used in Georgia.

29. Our study suggests several reasons why voters fail to verify BMD ballots. Most voters are unfamiliar with election technology, and many do not understand that the BMD printout *is* their legal ballot. Many Georgia voters may have this misconception, given the recent transition from DREs. Furthermore, most voters are not security experts and are unlikely to realize that it is possible for the printout to be different from what the BMD showed on screen. When asked by a poll worker, "Have you carefully reviewed each selection on your printed ballot?", one of our participants responded, "I checked it on the screen, it better be right." Among participants who *did* report errors, several believed *they* had made a mistake, even though the BMD really was cheating.

30. In a third part of our study, my coauthors and I provide a simple mathematical model for estimating how many voters will reports problems if BMDs are attacked in a way that changes an election outcome. The model assumes that the attacker will change both the barcode and the text, and it is likely to *overestimate* how strongly verification will protect against sophisticated attackers. However, it illustrates how weak a defense voter verification provides when all voters use BMDs.

31. Suppose there is a close election with an apparent margin of victory of 1% in favor of candidate A. If there had been no cheating, the result would have been a one-vote victory for candidate B, but an attacker hacked the BMDs so that they

misprinted a small fraction of the ballots. If voters report 14% of misprinted ballots (the rate my study found for top-of-the-ticket contests), then only about 1 in 1200 BMD voters will report a problem—roughly one per precinct—even though the election outcome is wrong due to fraud. This is likely far too few complaints to alert officials or the public that there was a major, outcome-determinative problem.

32. Election officials are unlikely to take disruptive actions, like a protracted and expensive forensic investigation, unless a much larger fraction of BMD voters report problems. Suppose officials would launch an investigation if more than 1% of BMD voters reported a problem. Under the scenario above, this condition would only be met if voters verified their ballots so carefully that they would report 67% of errors. This is ten times greater than the rate of error reporting we observed in our study.

33. Securing against misprinting attacks is much easier if only a small fraction of voters uses BMDs (without barcodes) and the rest use hand-marked paper ballots. This is because an attacker would be forced to cheat on a much larger fraction of BMD ballots in order to achieve the same level of fraud. In Maryland, which uses hand-marked paper ballots but makes BMDs available to voters who request them, about 2% of voters use BMDs. If only 2% of voters used BMDs in the scenario above, 1% of BMD voters would report a problem even if voters noticed only 3.8% of errors. Our results suggest that voters really do achieve this modest rate of verification

accuracy, even though it is unlikely they can achieve the far greater accuracy required when all voters use BMDs.

Reserving BMDs for Voters Request Them Would Strengthen Security

34. There is no practical sense in which "using BMDs only for voters with disabilities can create a greater risk to election security than using BMDs more broadly," as State Defendants claim.[20] To support this position, Defendants rely on the testimony of National Federation for the Blind President Mark Riccobono,[21] who has no discernable election security expertise. Mr. Riccobono posits that hacked BMDs would be less likely to be detected if only a small group of voters used them, particularly a group with many blind voters. This is incorrect, for several reasons:

(a) First, neither blind voters nor sighted voters can recognize an attack that changed only the barcodes, which are the only portion of the BMD printout that is counted in Georgia. So long as there are elections for which Georgia does not verify the outcome shown in the human-readable text of the ballots, such attacks would be potentially undetectable, and attackers would likely prefer to strike in this manner. Moreover, an attacker whose strategy was to target blind voters could

[20] Dckt. 658 at p. 17.
[21] Decl. of M. Riccobono (Dckt. 658-4) at 11.

do so even if all voters used BMDs. Malware running on the BMDs can easily detect whether a voter is using an assistive device like an audio ballot or a Braille keypad. An attacker could program the malware to cheat only for such voters.

(b) Second, to my knowledge, the rate of BMD error detection among blind voters has never been measured, but blind voters are not necessarily worse at ballot verification than the general population. Many people with visual impairments use portable devices to scan text and read it aloud. Such devices would allow blind voters to independently verify their printed ballots as well or better than sighted voters. Polling places could keep such devices on hand for voters who need them.

(c) Third, even if BMDs were reserved for voters who requested them, not all voters who used BMDs would be visually impaired. Some voters without disabilities would likely request to use the BMDs, as would voters with disabilities such as motor impairments that do not create any elevated difficulty for verification.

(d) Finally, using BMDs for all voters greatly magnifies security risks for everyone, including the blind, since all votes are potentially subject to manipulation by BMD malware, especially when they are counted from

> barcodes. Conversely, limiting the use of BMDs (without barcodes) to a smaller voter population reduces the risk than an attacker will strike at all, since such BMDs become a less appealing target. When BMD use is limited, an attacker would have to tamper with a larger fraction of BMD ballots in order to change election results by a particular amount. This makes it more likely that a noticeable fraction of BMD users will report errors than when the same number of misprinted ballots are distributed among the entire voting population. Furthermore, if the population of BMD users is smaller than the margin of victory, it will be impossible for a BMD-based attack to change the outcome.

35. Using BMDs for all voters has no practical security advantages compared to reserving BMDs for voters who request them. On the contrary, it makes BMDs a much more attractive target for attackers and leads to greatly increased risks for all voters—including the disabled—that their right to vote will be subverted by an attack on the BMDs. And regardless, there is no need for barcodes at all.

36. State Defendants argue that implementing HMBPs with a limited number of BMDs would violate the right to a secret ballot for voters with disabilities, because BMD ballots are distinguishable from hand-marked ballots, and some

precincts might have only one or a few voters with disabilities.[22] This risk can be mitigated easily by having poll workers encourage a small number of non-disabled voters in each precinct to use the BMDs (without barcodes). This would ensure that there was at least some minimum number of BMD votes in each precinct. And because BMD voters in such circumstances would still be a very small number among the total votes cast, they would not be an appealing target for attack and likely could not be outcome determinative in any event, as I explained above.

37. Mr. Riccobono discusses a variety of other problems that voters with disabilities sometimes encounter when BMDs are used infrequently.[23] These include poll workers who are unfamiliar with the machines and BMDs that are malfunctioning or not properly set up. These issues must be taken seriously, but they are solvable administrative deficiencies rather than intractable technological problems. They can be addressed through well designed training, testing, and inspection processes without exposing all voters, including voters with disabilities, to increased security risks.

[22] Dckt. 658 at p. 18.
[23] Riccobono decl. at 10.

Hand-Marked Paper Ballots Are Much More Secure than BMD Ballots, Especially Those with Barcodes

38. Hand-marked paper ballots (HMPBs) are the most widely used voting technology in the United States. They are widely used for in-person voting, and all 50 states, including Georgia, use them for absentee voting. When used with modern precinct-count optical scanners and rigorous RLAs, HMPBs can provide much stronger security than BMD-printed ballots, especially those based on barcodes.

39. Virtually every class of attack that affects HMPBs also affects BMDs, but BMDs—particularly those that use barcodes—additionally suffer from the serious possibility that malicious software will alter the voter's choices without detection. HMPBs can be well secured using existing election technology and procedural controls. In contrast, defending BMDs against cyberattacks relies on voters themselves to detect errors, which can be undetectable by voters, such as with barcode manipulation. When BMDs are used for all in-person voters, reliably detecting attacks would require far greater error detection accuracy than studies have shown voters achieve, even assuming they were capable of detecting the sorts of errors that can arise.

40. In comparing HMBPs to BMDs (generally, as opposed to barcode-based BMDs specifically), Defendants' expert Dr. Gilbert exaggerates the threat of what he

calls the "undervote hack"[24] and "overvote hack"[25]. He states that an attacker who gains physical access to hand-marked ballots could cast additional votes by adding marks in contests that voters left blank or could nullify votes by adding marks so that the votes are invalid. Furthermore, he states that "the only way to detect this attack would be to catch [the attacker] in the act."[26] These statements are misleading, for several reasons:

(a) BMD-printed ballots are vulnerable to very similar attacks. An attacker with physical access to the BMD printouts can use low-tech means to tamper with them. This could be as simple as discarding ballots that are unfavorable to the attacker, or as using a laser printer or a photocopier (neither an exotic technology) to generate additional ballots that are favorable to the attacker.

(b) There are already defenses in place to make physically tampering with the paper ballots difficult, and these protections would work as well for protecting HMBPs as they do for BMD-printed ballots. Georgia has procedures for safeguarding ballots during transportation and storage and for maintaining a chain of custody.

[24] Gilbert decl. at 37(C).
[25] Id. at 38(C).
[26] Id. at 37(C).

(c) Modern optical scanners such as Georgia's Dominion machines are designed to detect such fraud. They record a digital image of each ballot as it is scanned.[27] In the event that an audit found that the paper ballots and the scanner results disagreed, these digital images would reveal which ballots had been altered, and how. The attacks Dr. Gilbert is concerned about would result in a telltale pattern, such as marks made with similar handwriting or with a similar writing implement that all occurred in ballots that were stored in the same place. This would be strong evidence that a specific batch of ballots had been tampered with. Physical tampering would leave physical evidence on the ballots, and traditional police work would likely uncover the perpetrator.

(d) In contrast, if BMDs were infected with malware that altered a small fraction of the printed ballots, discovering the attack and identifying the attacker would potentially be difficult or impossible.

Additional Rebuttal of Declaration of Juan E. Gilbert[28]

41. Plaintiffs' expert Dr. Juan E. Gilbert is a computer scientist who specializes in human-centric computing. He is not an expert on computer security.

[27] Coomer decl. at 10.
[28] Gilbert decl. (Dckt. 658-3).

Nevertheless, I have responded to several of Dr. Gilbert's security-related assertions above, and I will address a few additional points here.

42. Dr. Gilbert expresses concerns about the possibility that voters will incorrectly mark HMPBs, leading to overvotes, undervotes, or miscounting.[29] However, the Dominion optical scanners used in Georgia are designed to combat these problems. If the scanners detect a potential error, they will warn the voter and give the voter the option of either casting the ballot as-is or correcting it.[30] This is analogous to the way that the BMDs provide warnings about undervotes on their review screens. Dr. Gilbert does not cite any data to show that undervotes, overvotes, or other errors remain frequent when voters are given an opportunity to correct them.

43. Dr. Gilbert acknowledges that optical scanners can be programmed to reject overvoted ballots but claims that this "could result in long lines and delayed voting at precincts when the voter has to re-mark a new ballot." Despite HMPBs

[29] Gilbert decl. at 37-39.

[30] This capability is described in Pennsylvania's examination of the Dominion system, available at https://www.dos.pa.gov/VotingElections/Documents/Voting Systems/Dominion Democracy Suite 5.5-A/Dominion Democracy Suite Final Report scanned with signature 011819.pdf:
"The ICP, precinct scanner of Democracy Suite 5.5 provides the voter with a caution message when the ballot contains errors, such as overvotes or undervotes. The voter is also presented an error report on the screen when the tabulator detects potential errors. The voter can either decide to affirm their intent by casting the ballot, or spoil the ballot and fill out another ballot."

being used as the primary means of recording votes in the majority of jurisdictions across the U.S., Dr. Gilbert cites no data to show that this really happens, and it is unlikely in a HMPB system. All a voter would need to correct an overvote is a new blank ballot, a writing implement, a surface on which to mark the ballot, and spot to do so privately. Moreover, only a small fraction of voters need to correct overvotes, so the overall effect on polling place throughput is likely to be small. By contrast, in an all-BMD system, having too few BMDs creates a bottleneck that will cause long lines—as does having BMDs that do not function properly.

44. Dr. Gilbert also expresses concerns about the potential for voters using HMPBs to mark ballots in a way that the scanners misreads or fails to recognize.[31] This is certainly possible, but, as stated above, Georgia's scanners will warn voters when an improper mark results in an overvote or undervote. In any event, a rigorous risk-limiting audit would detect and correct any error in an election outcome that resulted from the scanners interpreting the voter's marks differently than a human would. Although it is possible that some marks might be ambiguous even to humans, evidence from past elections shows that such marks are extremely rare. During the

[31] Gilbert decl. at 39(A).

2008 Minnesota Senate recount, only 14 ballots out of 2.9 million resulted in disagreement among canvassers about the voter's intent.[32]

45. Dr. Gilbert claims that a BMD barcode can be "examined during pre-election testing or post-election audits or recounts to confirm its validity."[33] This is misleading: although the barcodes on individual test ballots could be confirmed during testing, that has limited relevance to the ballots voters cast during the election. BMD malware would likely be programmed to cheat on only a fraction of barcodes, and an attacker could rely on other features such as the date and time or the number of times the BMD had been used to conceal cheating during testing.

46. Dr. Gilbert states that "a hand-marked paper ballot system is not accessible to voters with disabilities while a BMD system is."[34] However, I do not understand Curling Plaintiffs to be challenging the use of appropriate BMDs by voters with disabilities. The security risks of using BMDs are much greater when they are used by all voters, especially with barcodes. Using HMPBs for most voters while providing BMDs (without barcodes) for voters who request them would result in no

[32] "Minnesota's Historic 2008 Election" (2009), available at https://www.sos.state.mn.us/media/3078/minnesotas-historic-2008-election.pdf.
[33] Gilbert decl. at 39(E).
[34] Id. 40.

loss of accessibility but would reduce BMD security risks for all voters, including voters with disabilities.

47. Dr. Gilbert states that it is, in his opinion, "unacceptable" that "proponents of hand-marked paper ballots while arguing that BMDs are insecure suggest that it is OK for people with disabilities to vote on [them]."[35] I am uncertain what he means by this, because he concedes that "generally any computer can be hacked",[36] and he clearly believes that it is acceptable for people with disabilities to use computer-based BMDs. In my opinion, despite their security risks, appropriate BMDs (without barcodes) are the most secure category of voting technology now available for use by voters with certain disabilities. However, when all voters use BMDs, as in Georgia, they create a serious risk that outcome-changing cyberattacks will go undetected. Barcodes needlessly exacerbate this already serious risk.

48. Dr. Gilbert estimates that around 635,000 disabled voters cast votes in Georgia in 2016.[37] This does not imply that anywhere near that many voters require the assistance of a BMD to vote. The statistics Dr. Gilbert cites include voters with many kinds of disabilities, including ones that impact mobility but do not inhibit the private use of HMPBs. A better way to estimate the population that needs BMDs is

[35] Id. at 40(C).
[36] Id. at 44.
[37] 40(E)

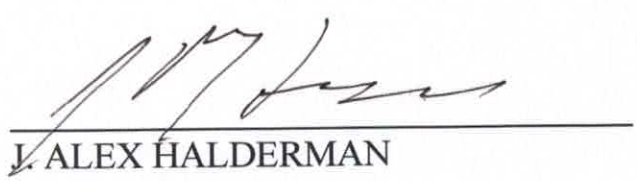
to look to states that use HMPBs and make BMDs available to votes upon request. One such state is Maryland. The National Federation of the Blind of Maryland cites data from the Maryland State Board of Election showing that, during the 2016 General Election, only 1.8% of Maryland voters used BMDs.[38] There were 4.1 million ballots cast during the 2016 General election in Georgia, which implies that about 75,000 Georgia voters would have used BMDs, if Georgia voters used them at the same rate as Maryland voters. This is by no means an insignificant number of people, but nonetheless it is much smaller than Dr. Gilbert's data might imply.

49. Defendants incorrectly ascribe to Dr. Gilbert the proposition that "research shows that voters will verify their ballots when posted instructions are given, such as those required by H.B. 316."[39] Dr. Gilbert, citing unpublished research by Dr. Michael Byrne, says only that *having a poll worker prompt voters* to review their ballots increases verification.[40] My own peer-reviewed study discussed above is in agreement that certain kinds of verbal prompts by poll workers can have a modest positive effect, but it finds no statistically significant increase in verification from signage reminding voters to verify their ballots, which is what H.B. 316 requires. And again, as I explained above, voter verification cannot reliably detect various

[38] https://elections.maryland.gov/about/meeting_materials/October_2017.pdf
[39] Dckt. 658 at p. 11.
[40] Gilbert decl. at 51.

attacks on BMDs, especially when barcodes that voters cannot read are used to tabulate votes.

I declare under penalty of the perjury laws of the State of Georgia and the United States that the foregoing is true and correct and that this declaration was executed this 16th day of December, 2019 in Ann Arbor, Michigan.



J. ALEX HALDERMAN